Discussiones Mathematicae
Graph Theory 20 (2000) 5–21

COLOURING OF CYCLES IN THE DE BRUIJN GRAPHS

Ewa Łazuka and Jerzy Żurawiecki

Department of Applied Mathematics
Technical University of Lublin
Bernardyńska 13, 20–950 Lublin, POLAND

e-mail: elazuka@antenor.pol.lublin.pl
e-mail: zuraw@antenor.pol.lublin.pl

Abstract

We show that the problem of finding the family of all so called *the locally reducible factors* in the binary de Bruijn graph of order k is equivalent to the problem of finding all colourings of edges in the binary de Bruijn graph of order $k-1$, where each vertex belongs to exactly two cycles of different colours. In this paper we define and study such colouring for the greater class of the de Bruijn graphs in order to define a class of so called *regular factors,* which is not so difficult to construct. Next we prove that each locally reducible factor of the binary de Bruijn graph is a subgraph of a certain regular factor in the m-ary de Bruijn graph.

Keywords: the de Bruijn graph, decomposition, colouring of edges in a cycle, factors of the de Bruijn graph, locally reducible factor, feedback function, locally reducible function.

1991 Mathematics Subject Classification: 05C15, 05C20, 05C38, 05C45, 94A55.

1 Introduction

The binary de Bruijn graph of order k is a directed Euler graph with 2^k vertices and 2^{k+1} edges, in which for each vertex exactly two edges are incident into and exactly two edges are incident out of. Because of numerous applications the de Bruijn graphs have been studied in many papers, most of which deal with the problem of constructing Hamiltonian cycles [3] which are used to design and analyse cryptographic systems [2], [4], [5], [8]. Most frequently known algorithms for finding the Hamiltonian cycles in the

de Bruijn graph construct such the cycles by joining the cycles of one from among its maximal subgraphs consisting of vertex disjoint cycles. Such subgraphs are called *factors.* The efficiency of the algorithm is determined both by a choice of a suitable factor and by a way of joining its cycles. Therefore it is necessary to see connections between the factors. In the paper [7] a certain order in the family of the factors of the de Bruijn graph was studied. Here the factors forming the Hamiltonian cycles are the maximal elements and *locally reducible factors* defined in [11] are the minimal elements. The locally reducible factors are sufficient to determine, by means of the algorithm presented in [9], all the Hamiltonian cycles. On the other hand, in the de Bruijn graph of order k the cycles of the locally reducible factors are determined by the cycles of the de Bruijn graph of order $k-1$ in such a way that a sequence of succeding vertices of each cycle in the locally reducible factor is a sequence of succeding edges in a certain cycle of the de Bruijn graph of order $k-1$. The construction of all locally reducible factors in the de Bruijn graph of order k and next of all maximal chains (according to the order considered in [7]) containing a certain factor forming the Hamiltonian cycle in this graph allow to give a detailed description of its structure. It is very important for the mentioned problem of the construction and the analysis of the cryptographic systems [8]. However finding the effective way to construct all the locally reducible factors remains an open problem.

The problem of finding the family of all the locally reducible factors in the binary de Bruijn graph of order k is equivalent to the the problem of finding all colourings of edges in the binary de Bruijn graph of order $k-1$, where each vertex belongs to exactly two cycles of different colours. In this paper we define and study such colouring for the greater class of the de Bruijn graphs in order to define a class of so called *regular factors,* which is not so difficult to construct. Next we prove that each locally reducible factor of the binary de Bruijn graph is a subgraph of a certain regular factor in the de Bruijn graph with the vertices from the set $\{0,1,\ldots,m-1\}^k$, where $m>1$. There exist important circumstances confirming that it is sufficient to consider the factors of the de Bruijn graph for $m=4$ to obtain all of the regular factors of order k proving the locally reducible factors of order k. Unfortunately we are not able to prove or refute this hypothesis.

2. The de Bruijn Graph and its Factors

The *m-ary de Bruijn graph of order k* is a directed graph $B_k^{(m)}$ with elements

of $\{0,1,\ldots,m-1\}^k$ as the vertices, where exactly m edges are incident out of a vertex $(v_1,v_2,\ldots,v_k)$ and each of them is incident into one of the vertices $(v_2,\ldots,v_k,0),\ldots,(v_2,\ldots,v_k,m-1)$. Moreover exactly m edges are incident into a vertex $(v_1,v_2,\ldots,v_k)$ and each of them is incident out of one of the vertices $(0,v_1,\ldots,v_{k-1}),\ldots,(m-1,v_1,\ldots,v_{k-1})$. As the edge incident out of the vertex $(v',v_2,\ldots,v_k)$ into the vertex $(v_2,\ldots,v_k,v'')$ can be identified with $(v',v_2,\ldots,v_k,v'')\in\{0,1,\ldots,m-1\}^{k+1}$ and conversely, then $B_{k+1}^{(m)}$ is the edge graph of $B_k^{(m)}$.

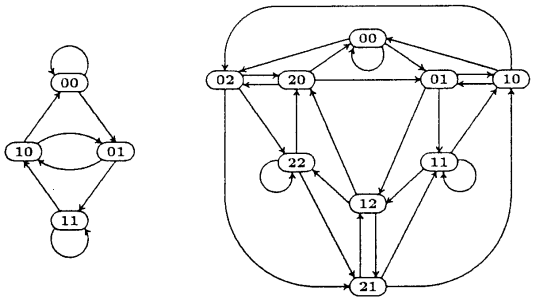


Figure 2.1. The graphs $B_2^{(2)}$ and $B_2^{(3)}$

Let $Z_m=\{0,1,\ldots,m-1\}$ and let $\mathcal{C}_{(m)}^k$ denote the family of all such functions $\varphi\colon Z_m^k\to Z_m$ that

$$(2.1)\qquad if\quad a\neq b\quad then\quad \varphi(a,x_2,\ldots,x_k)\neq\varphi(b,x_2,\ldots,x_k)$$

for any elements a and b from Z_m and for $(x_2,\ldots,x_k)\in Z_m^{k-1}$. Each function from $\mathcal{C}_{(m)}^k$ is called a *feedback function.* Each $\varphi\in\mathcal{C}_{(m)}^k$ determines the maximal subgraph $B_k^{(m)}[\varphi]$ of $B_k^{(m)}$ composed of disjoint directed cycles in which an arbitrary edge is incident out of a vertex $(v_1,v_2,\ldots,v_k)$ into a vertex $(v_2,\ldots,v_k,\varphi(v_1,v_2,\ldots,v_k))$. The graph $B_k^{(m)}[\varphi]$ is said to be the *factor of* $B_k^{(m)}$ *corresponding to* φ.

Since $B_k^{(m)}$ is the edge graph of $B_{k-1}^{(m)}$, then each cycle G of $B_k^{(m)}[\varphi]$ corresponds to a subgraph G' of $B_{k-1}^{(m)}$ in such a way that the edges of G' are

the vertices of G. The graph G' is an Euler graph because it forms a closed walk in $B_{k-1}^{(m)}$. It is called the *projection of the cycle G onto the graph $B_{k-1}^{(m)}$*.

For an arbitrary $\varphi \in \mathcal{C}_{(m)}^{k}$ we shall consider the family $B_k^{\bullet}[\varphi]$ of the projections of all cycles of the factor $B_k^{(m)}[\varphi]$ onto $B_{k-1}^{(m)}$. This family is called the *decomposition of the graph $B_{k-1}^{(m)}$ determined by the factor $B_k^{(m)}[\varphi]$*. In order to mark the decomposition $B_k^{\bullet}[\varphi]$ of $B_{k-1}^{(m)}$ we colour the edges of $B_{k-1}^{(m)}$ with the colours from the set $\{1, 2, \ldots, t\}$ in the following way:

(2.2) the edges of $B_{k-1}^{(m)}$ which form the projection of a cycle of $B_k^{(m)}[\varphi]$, are coloured with the same colour,

(2.3) if the projections of the different cycles of $B_k^{(m)}[\varphi]$ have a common vertex then the edges of these projections are coloured with the different colours.

The graph $B_{k-1}^{(m)}$ the edges of which are coloured according to the rules described above with the minimal number of colours, is called an *undirected projection of the factor $B_k^{(m)}[\varphi]$ onto the graph $B_{k-1}^{(m)}$*. If exactly t colours have been used to form the undirected projection of $B_k^{(m)}[\varphi]$ onto $B_{k-1}^{(m)}$, then such a projection is called *t-chromatic,* while the number t is called the *chromatic number of the projection.* Of course $t \geq m$ and each factor may have many undirected projections (with the same chromatic number) which depend on the way of the colouring of the edges in the cycles.

There may exist many factors determining the same decomposition. Their number depends on how many different closed Euler walks may be obtained in each graph forming the family $B_k^{\bullet}[\varphi]$. As an example we can consider the family of the factors composed of the Hamiltonian cycles. Each of them corresponds to the decomposition consisting of the only one element, namely the graph $B_{k-1}^{(m)}$. There exist also factors of $B_k^{(m)}$ which determine the decompositions of $B_{k-1}^{(m)}$ uniquely. It occurs if and only if there exists exactly one closed Euler walk in each graph from the family $B_k^{\bullet}[\varphi]$. For instance, it is fullfilled by the factors the projections of which contain only the cycles. They are called *locally reducible factors* and the corresponding functions — *locally reducible functions* [11]. If the projection of the locally reducible factor $B_k^{(m)}[\varphi]$ is t-chromatic then the function φ is called *t-reducible.*

Theorem 2.1. *A feedback function φ is locally reducible if and only if no cycle of the factor $B_k^{(m)}[\varphi]$, which contains a vertex $(v_1, v_2, \ldots, v_k)$, does not contain such a vertex $(\tilde{v}_1, v_2, \ldots, v_k)$ that $v_1 \neq \tilde{v}_1$.*

Proof. The projection of the cycle of the factor $B_k^{(m)}[\varphi]$ which contains a vertex $(x_1, \ldots, x_k)$ is the subgraph of $B_{k-1}^{(m)}$ which has the edge $(x_1, \ldots, x_k)$ incident into the vertex $(x_2, \ldots, x_k)$. The projections of the cycles containing the vertices $(v_1, v_2, \ldots, v_k)$ and $(\tilde{v}_1, v_2, \ldots, v_k)$ respectively, have the common vertex $(v_2, \ldots, v_k)$ in the graph $B_{k-1}^{(m)}$. Thus, if $v_1 \neq \tilde{v}_1$ then they are the cycles if and only if the projected cycles are different. ■

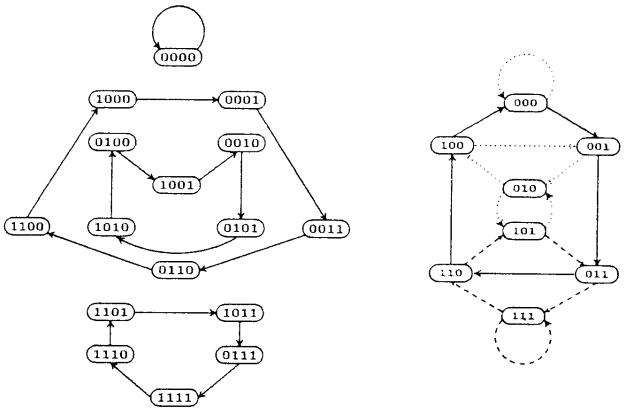


Figure 2.2. The factor $B_4^{(2)}[\varphi]$ and its undirected projection onto the graph $B_3^{(2)}$, where $\varphi(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4$ in $GF(2)$

If φ is a t-reducible function, then each t-chromatic, undirected projection of $B_k^{(m)}[\varphi]$ onto $B_{k-1}^{(m)}$ determines the family $\{\varphi_1, \varphi_2, \ldots, \varphi_t\}$, which consists of the partial functions from Z_m^{k-1} to Z_m satisfying the following condition

(2.4) the edge $(e_1, \ldots, e_k)$ of $B_{k-1}^{(m)}$ is of the colour $i \in \{1, \ldots, t\}$ if and only if the equality $\varphi_i(e_1, \ldots, e_{k-1}) = e_k$ holds.

It is called a *colouring family of* $B_{k-1}^{(m)}$ *determined by the locally reducible function* φ.

Theorem 2.2. *A family* $\{\varphi_1, \ldots, \varphi_t\}$ *of partial functions from* Z_m^{k-1} *to* Z_m *is the colouring family determined by a locally reducible function if and only if it is the minimal* (*considering a number of elements*) *family satisfying the following conditions:*

(2.5) *if* $(x_1, \ldots, x_{k-1}) \in Dom(\varphi_i)$, *then* $(x_2, \ldots, x_{k-1}, \varphi_i(x_1, \ldots, x_{k-1})) \in Dom(\varphi_i)$,

(2.6) *if for* $a \neq b$ *the condition* $\{(a, x_2, \ldots, x_{k-1}), (b, x_2, \ldots, x_{k-1})\} \subseteq Dom(\varphi_i)$ *holds, then* $\varphi_i(a, x_2, \ldots, x_{k-1}) \neq \varphi_i(b, x_2, \ldots, x_{k-1})$,

(2.7) *for each* $x \in Z_m^{k-1}$ *such a maximal family* (*considering the relation* $\subseteq$) $\mathcal{F}_x \subseteq \{\varphi_1, \ldots, \varphi_t\}$ *that*

$$x \in \bigcap_{\xi \in \mathcal{F}_x} Dom(\xi)$$

consists of exactly m *elements and for any different functions* ξ' *and* ξ'' *from* $\mathcal{F}_x$ *it is true that* $\xi'(x) \neq \xi''(x)$.

Proof. *Necessity.* Let us assume that $\{\varphi_1, \ldots, \varphi_t\}$ is a colouring family, which colours $B_{k-1}^{(m)}$, determined by a locally reducible function φ.

In order to prove (2.5) let us note that according to (2.2) if an edge $(e_1, e_2, \ldots, e_k)$ of $B_{k-1}^{(m)}$ is of the colour i, then one of the edges of the form $(e_2, \ldots, e_k, e')$ has also the same colour. It follows from (2.4) that

$$e_k = \varphi_i(e_1, \ldots, e_{k-1}) \quad \text{and} \quad e' = \varphi_i(e_2, \ldots, e_k)$$

which imply $(e_2, \ldots, e_{k-1}, \varphi_i(e_1, \ldots, e_{k-1})) \in \mathrm{Dom}(\varphi_i)$.

In order to prove (2.6) let us consider an arbitrary edge $(e_0, e_1, \ldots, e_{k-1})$ of $B_{k-1}^{(m)}$ which is incident into a vertex $(e_1, \ldots, e_{k-1})$. According to (2.4) there exists a function φ_i satisfying the equality $e_{k-1} = \varphi_i(e_0, e_1, \ldots, e_{k-2})$. Furthermore, it follows from the condition (2.3) that for none of other edges $(\tilde{e}_0, e_1, \ldots, e_{k-1})$ incident into the vertex $(e_1, \ldots, e_{k-1})$ this equality holds and this way the condition (2.6) is proved.

The condition (2.7) results from the fact that exactly m edges are incident into each vertex, so there exist exactly m cycles of different colours which contain this vertex.

The condition (2.7) and the t-reducibility of φ imply that the correspondence between the edges incident out of a fixed vertex of $B_{k-1}^{(m)}$ (according to the condition (2.4)) and one of the functions from $\{\varphi_1, \ldots, \varphi_t\}$ is one-to-one. And so we have that the considering family is minimal.

Sufficiency. Let us consider an arbitrary minimal family $\{\varphi_1, \ldots, \varphi_t\}$ which satisfies the conditions (2.5), (2.6) and (2.7). We colour the edges of $B_{k-1}^{(m)}$ in the following way: the edge $(e_1, \ldots, e_{k-1}, e_k)$ incident out of the vertex $(e_1, \ldots, e_{k-1})$ is of the colour i if and only if $e_k = \varphi_i(e_1, \ldots, e_{k-1})$. It follows from (2.7) that each from among m edges incident out of this vertex has different colour. From (2.6) we have that each from among m edges

incident into this vertex is of different colour, which according to the condition (2.5) is one of m colours colouring the edges which are incident out of. Therefore each vertex of $B_{k-1}^{(m)}$ belongs to m cycles of different colours and the graph coloured in this way is an undirected projection of $B_k^{(m)}[\varphi]$ onto the graph $B_{k-1}^{(m)}$, where

$$(2.8)\quad \varphi(x_1,x_2,\ldots,x_k)=\begin{cases}\varphi_1(x_2,\ldots,x_k), & \text{if } (x_1,\ldots,x_{k-1})\in Dom(\varphi_1)\\ & \text{and } x_k=\varphi_1(x_1,\ldots,x_{k-1}),\\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\\ \varphi_t(x_2,\ldots,x_k), & \text{if } (x_1,\ldots,x_{k-1})\in Dom(\varphi_t)\\ & \text{and } x_k=\varphi_t(x_1,\ldots,x_{k-1}).\end{cases}$$

That completes the proof of this theorem. ∎

A minimal family $\{\varphi_1,\ldots,\varphi_t\}$ of partial functions from Z_m^{k-1} to Z_m, which satisfies the conditions (2.5), (2.6) and (2.7) mentioned in Theorem 2.2, is called a *colouring family.*

For an arbitrary colouring family $\{\varphi_1,\ldots,\varphi_t\}$ the symbol ${}^{\mathrm{ex}}\{\varphi_1,\ldots,\varphi_t\}$ will denote the function $\varphi\in\mathcal{C}_{(m)}^k$ defined by the condition (2.8), called the *extension of the colouring family* $\{\varphi_1,\ldots,\varphi_t\}$.

Corollary 2.1. *If a partial functions $\varphi_1,\ldots,\varphi_t$ form the colouring family then the function ${}^{\mathrm{ex}}\{\varphi_1,\ldots,\varphi_t\}$ is locally reducible.*

The above corollary allows for constructing the locally reducible function in the case if the colouring family is given. Unfortunately no simple algorithm is known for finding the colouring family unless its elements are the total functions. We shall study this special case in the next part of the paper.

3. Regular Functions

In some cases the functions $\varphi_1,\varphi_2,\ldots,\varphi_t$ forming a colouring family might be total functions. Then the function $\varphi={}^{\mathrm{ex}}\{\varphi_1,\ldots,\varphi_t\}$ is called a *regular function,* its factor $B_k^{(m)}[\varphi]$ — *a regular factor* and the functions $\varphi_1,\varphi_2,\ldots,\varphi_t$ are called *components of* φ.

Theorem 3.1. *A locally reducible function ${}^{\mathrm{ex}}\{\varphi_1,\ldots,\varphi_t\}$ is regular if and only if $t=m$.*

Proof. *Necessity.* For each vertex of $B_{k-1}^{(m)}$ there are exactly m edges incident into and exactly m edges incident out of this vertex. Since the function $\varphi = {}^{\mathrm{ex}}\{\varphi_1, \ldots, \varphi_t\}$ is regular, the colouring family $\{\varphi_1, \ldots, \varphi_t\}$ consists of only total functions. For any vertex of $B_{k-1}^{(m)}$ each of them colours exactly one edge from among m edges incident into and exactly one edge from among m edges incident out of this vertex. Thus the equation $m = t$ must be satisfied.

Sufficiency. The condition $t = m$ concerning $\varphi = {}^{\mathrm{ex}}\{\varphi_1, \ldots, \varphi_t\}$ means that each of its components is total, so φ is a regular function. ∎

Example 3.1. We shall prove that the function $\vartheta\colon Z_m^k \to Z_m$ definied by the condition

$$\vartheta(x_1, \ldots, x_k) = x_1$$

is m-reducible for each $m > 1$, so it is a regular fuction. In order to prove this we consider a function $f\colon Z_m^k \to Z_m$ such that $f(x_1, x_2, \ldots, x_k)$ is the residual of the division of the sum $x_1 + x_2 + \cdots + x_k$ by m. Let us note that

$$f(x_1, x_2, \ldots, x_k) = f(x_2, \ldots, x_k, x_1) = f(x_2, \ldots, x_k, \vartheta(x_1, x_2, \ldots, x_k))$$

and it follows from this equality that f is the function determining the same colour for all vertices of the same cycle in $B_k^{(m)}[\vartheta]$. On the other hand, for each $(x_1, x_2, \ldots, x_k) \in Z_m^k$, if $\tilde{x}_1 \in Z_m \setminus \{x_1\}$ then we have the inequality $f(x_1, x_2, \ldots, x_k) \neq f(\tilde{x}_1, x_2, \ldots, x_k)$. Then f restricted to the set $\{(0, x_2, \ldots, x_k), (1, x_2, \ldots, x_k), \ldots, (m-1, x_2, \ldots, x_k)\}$ is one-to-one function in Z_m. Therefore the cycles which contain the vertices $(x_1, x_2, \ldots, x_k)$ and $(\tilde{x}_1, x_2, \ldots, x_k)$ respectively, have the different colours. Finally, the function f defines an undirected, m-chromatic projection of $B_k^{(m)}[\vartheta]$ onto $B_{k-1}^{(m)}$ in which each vertex of $B_{k-1}^{(m)}$ belongs to one from among m cycles of different colours. Then ϑ is a regular function.

The construction of regular functions is not too difficult because the family $\{\varphi_1, \ldots, \varphi_m\}$ formed by the functions from the set $\mathcal{C}_{(m)}^{k-1}$ is the colouring family if and only if for each $x \in Z_m^{k-1}$ the following condition holds

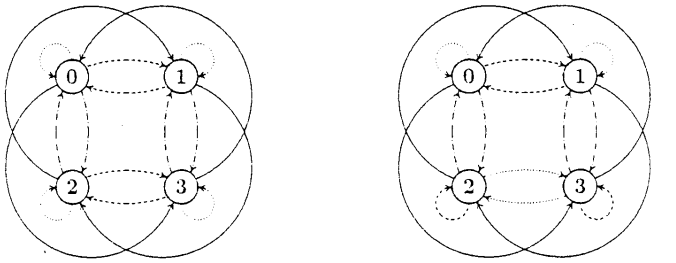
$$\textit{if } i \neq j, \textit{ then } \varphi_i(x) \neq \varphi_j(x). \tag{3.1}$$

It can be written in another form as $B_{k-1}^{(m)} = \bigcup_{\tau \in \{\varphi_1, \ldots, \varphi_m\}} B_{k-1}^{(m)}[\tau]$.

Then the definition of the function $\varphi = {}^{\mathrm{ex}}\{\varphi_1, \ldots, \varphi_m\}$ is of the form

$$\varphi(x_1, x_2, \ldots, x_k) = \begin{cases} \varphi_1(x_2, \ldots, x_k), & if\ x_k = \varphi_1(x_1, \ldots, x_{k-1}), \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \varphi_m(x_2, \ldots, x_k), & if\ x_k = \varphi_m(x_1, \ldots, x_{k-1}). \end{cases}$$

There may exist the different colouring families which define the same regular function. Such a situation is showed in Figure 3.1, and the following theorem states the connection between these families.



x	$\delta_1(x)$	$\delta_2(x)$	$\delta_3(x)$	$\delta_4(x)$
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

x	$\delta'_1(x)$	$\delta'_2(x)$	$\delta'_3(x)$	$\delta'_4(x)$
0	0	1	2	3
1	1	0	3	2
2	3	2	0	1
3	2	3	1	0

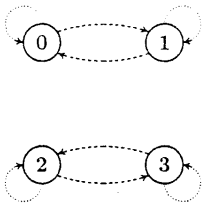


Figure 3.1. The illustration of Theorem 3.2: the graph $B_1^{(4)}$ coloured by the families $\{\delta_1, \delta_2, \delta_3, \delta_4\}$ and $\{\delta'_1, \delta'_2, \delta'_3, \delta'_4\}$ respectively, and its disconnected subgraph $B_1^{(4)}[\delta_1] \cup B_1^{(4)}[\delta_2]$

Theorem 3.2. *For any colouring families* $\{\varphi_1, \ldots, \varphi_m\}$ *and* $\{\psi_1, \ldots, \psi_m\}$ *which colour the graph* $B_{k-1}^{(m)}$, *if* ${}^{\mathrm{ex}}\{\varphi_1, \ldots, \varphi_m\} = {}^{\mathrm{ex}}\{\psi_1, \ldots, \psi_m\}$ *then the equality* $\{\varphi_1, \ldots, \varphi_m\} = \{\psi_1, \ldots, \psi_m\}$ *holds if and only if for any functions* φ' *and* φ'' *from* $\{\varphi_1, \ldots, \varphi_m\}$ *the graph* $B_{k-1}^{(m)}[\varphi'] \cup B_{k-1}^{(m)}[\varphi'']$ *is connected.*

Proof. *Necessity.* We shall prove that if for a regular function δ there exists a colouring family $\{\delta_1, \delta_2, \ldots, \delta_m\}$ such that the graph $B_{k-1}^{(m)}[\delta_1] \cup B_{k-1}^{(m)}[\delta_2]$

is not connected, then there also exists a colouring family $\{\delta'_1, \delta'_2, \ldots, \delta'_m\}$ such that

$$\{\delta_1, \delta_2, \ldots, \delta_m\} \neq \{\delta'_1, \delta'_2, \ldots, \delta'_m\}$$

and

$$^{\mathrm{ex}}\{\delta_1, \delta_2, \ldots, \delta_m\} = {}^{\mathrm{ex}}\{\delta'_1, \delta'_2, \ldots, \delta'_m\}.$$

Let us assume that the graph $B^{(m)}_{k-1}[\delta_1] \cup B^{(m)}_{k-1}[\delta_2]$ is not connected and consider the subset D of the set $\{0,1\}^{k-1}$ consisting of the vertices of one of the components of $B^{(m)}_{k-1}[\delta_1] \cup B^{(m)}_{k-1}[\delta_2]$. Of course $D \neq \{0,1\}^{k-1}$, so we only need to put

$$\delta'_1(x) = \begin{cases} \delta_1(x) & \text{for } x \in \{0,1\}^{k-1} \setminus D, \\ \delta_2(x) & \text{for } x \in D, \end{cases}$$

$$\delta'_2(x) = \begin{cases} \delta_2(x) & \text{for } x \in \{0,1\}^{k-1} \setminus D, \\ \delta_1(x) & \text{for } x \in D, \end{cases}$$

and $\delta'_3 = \delta_3, \ldots, \delta'_m = \delta_m$ to receive the colouring family we have looked for.

Sufficiency. We shall prove that if for any regular function δ there exists the colouring family $\{\delta_1, \delta_2, \ldots, \delta_m\}$ such that each graph from among the graphs of the form $B^{(m)}_{k-1}[\delta_1] \cup B^{(m)}_{k-1}[\delta']$ for $\delta' \in \{\delta_2, \ldots, \delta_m\}$ is connected, then $\{\delta_1, \delta_2, \ldots, \delta_m\}$ is the only family (with reference to the order) colouring the graph $B^{(m)}_{k-1}$ corresponding to the function δ.

Let us consider any colouring family $\{\delta'_1, \ldots, \delta'_m\}$ for which the equality

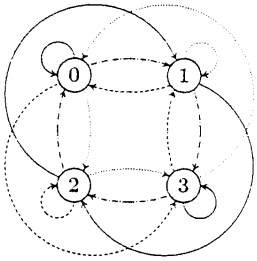
$$^{\mathrm{ex}}\{\delta_1, \delta_2, \ldots, \delta_m\} = {}^{\mathrm{ex}}\{\delta'_1, \delta'_2, \ldots, \delta'_m\}$$

holds. If we assume $\{\delta_1, \delta_2, \ldots, \delta_m\} \neq \{\delta'_1, \delta'_2, \ldots, \delta'_m\}$ then there exist the positive integers i and j and also the nonempty, proper subset D of Z^{k-1}_m such that

$$\delta_i(x) = \delta'_j(x) \text{ for } x \in Z^{k-1}_m \setminus D \qquad \textit{and} \qquad \delta_i(x) \neq \delta'_j(x) \text{ for } x \in D.$$

It means that the cycles of the factors $B^{(m)}_{k-1}[\delta_i]$ and $B^{(m)}_{k-1}[\delta'_j]$ with the vertices from the set $Z^{k-1}_m \setminus D$ are identical, however other cycles of these factors are different. Without loss of generality we can assume that D is the minimal set of this property, i.e. there does not exist the colouring family which defines the set smaller than D in the above way. Let δ_s be such a function from the set $\{\delta_2, \ldots, \delta_m\}$ that the factors $B^{(m)}_{k-1}[\delta_s]$ and $B^{(m)}_{k-1}[\delta'_s]$ have a common

cycle formed by the vertices from D. The assumption that D is minimal causes that all cycles of both factors, which have the vertices from D, are identical. It means next that in the graph $B_{k-1}^{(m)}[\delta_1] \cup B_{k-1}^{(m)}[\delta_s]$ all vertices of each cycle having at least one vertex from D, are also the elements of D. Finally it lets us draw the conclusion that the graph we have considered is not connected. ■



$^{ex}\{\delta_1, \delta_2, \delta_3, \delta_4\}$:

$$\begin{cases} 00 \to 0 \\ 01 \to 3 \\ 02 \to 3 \\ 03 \to 1 \\ 10 \to 3 \\ 11 \to 1 \\ 12 \to 1 \\ 13 \to 2 \\ 20 \to 1 \\ 21 \to 2 \\ 22 \to 2 \\ 23 \to 0 \\ 30 \to 2 \\ 31 \to 0 \\ 32 \to 0 \\ 33 \to 3 \end{cases}$$

x	$\delta_1(x)$	$\delta_2(x)$	$\delta_3(x)$	$\delta_4(x)$
0	1	3	2	0
1	3	0	1	2
2	0	2	3	1
3	2	1	0	3

Figure 3.2. The graph $B_1^{(4)}$ uniquely coloured by the family $\{\delta_1, \delta_2, \delta_3, \delta_4\}$

In the case $m = 2$, which was examined in detail in [10], the regular functions were called *elementary functions*. The theory of such functions is particularly simple. Let us namely note that for each function $\psi \in \mathcal{C}_{(2)}^{k-1}$ there exists exactly one function $\bar{\psi}$ such that

$$\bar{\psi}(x) \neq \psi(x) \quad \text{for } x \in \{0,1\}^{k-1}.$$

Therefore we can denote the regular function ${}^{\mathrm{ex}}\{\psi, \bar{\psi}\}$ by the symbol ${}^{\mathrm{ex}}\psi$ or ${}^{\mathrm{ex}}\bar{\psi}$. Moreover it is true that

$$(3.2)\quad {}^{\mathrm{ex}}\psi(x_1,\dots,x_k) = \psi(x_1,\dots,x_{k-1}) + \psi(x_2,\dots,x_k) + x_k \quad \textit{in } GF(2).$$

For instance, if $\psi(x_1,\dots,x_{k-1}) = x_1 + x_2 + \cdots + x_{k-1}$, then

$${}^{\mathrm{ex}}\psi(x_1,\dots,x_{k-1}) = (x_1 + x_2 + \cdots + x_{k-1}) + (x_2 + x_3 + \cdots + x_k) + x_k = x_1.$$

And so the function $\vartheta \in \mathcal{C}^k_{(2)}$ defined by the equality $\vartheta(x_1, x_2, \dots, x_k) = x_1$ is the regular function.

For $k = 3$ the only regular functions are $\varphi_1(x_1, x_2, x_3) = x_1 + x_2 + x_3$ and $\varphi_2(x_1, x_2, x_3) = x_1$. For $k = 4$ all regular functions can be formed with the use of the operation ${}^{\mathrm{ex}}$ to each function from any family consisting of eight functions from $\mathcal{C}^3_{(2)}$ which does not contain both ψ and $\bar{\psi}$.

If we identify the function φ with a certain polynomial from the ring $GF(2)[x_1,\dots,x_k]$, then we can give the criterion which lets us decide if φ is the regular function or not.

Theorem 3.3 ([10], Theorem 6.3)**.** *A feedback function φ defined by the equality*

$$\varphi(x_1,\dots,x_k) = x_1 + x_2 f_2(x_3,\dots,x_k) + \cdots + x_{k-1} f_{k-1}(x_k) + x_k f_k + f_{k+1}$$

is regular if and only if the following conditions hold:

(i) $f_{k+1} = 0$,

(ii) $f_2(x_1,\dots,x_{k-2}) + \cdots + f_{k-1}(x_1) + f_k = 0$ *for all* $(x_1,\dots,x_{k-1}) \in \{0,1\}^{k-1}$.

For instance, if $\varphi(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2(x_3 + x_4) + x_3(x_4 + x_5) + x_4 + x_5$ then $f_2(x_1, x_2, x_3) = x_1 + x_2 = f_3(x_1, x_2)$ and $f_4(x_1) = f_5 = 1$. It means that the function φ is regular. A very simple criterion for the locally reducible functions to be regular can be obtained for the binary linear functions.

If $\varphi(x_1,\dots,x_k) = x_1 + c_2x_2 + \cdots + c_kx_k$ then φ is the regular function if and only if in $GF(2)$ the equality $c_2 + \cdots + c_k = 0$ holds, i.e., if the polynomial representing the function φ is of an odd number of nonzero coefficients. This condition is satisfied by the function $\vartheta(x_1, x_2, \dots, x_k) = x_1$.

The regular functions will be used to study a general case of the locally reducible functions. First we have to define a *subfactor.*

The subgraph of a factor $B^{(m)}_k[\varphi]$ which is a factor of $B^{(t)}_k$ will be called a *t-subfactor* of $B^{(m)}_k[\varphi]$ or a *subfactor* if the value of the parameter t is defined by the preceding assumptions. In particular a 2-subfactor is called a *binary subfactor.*

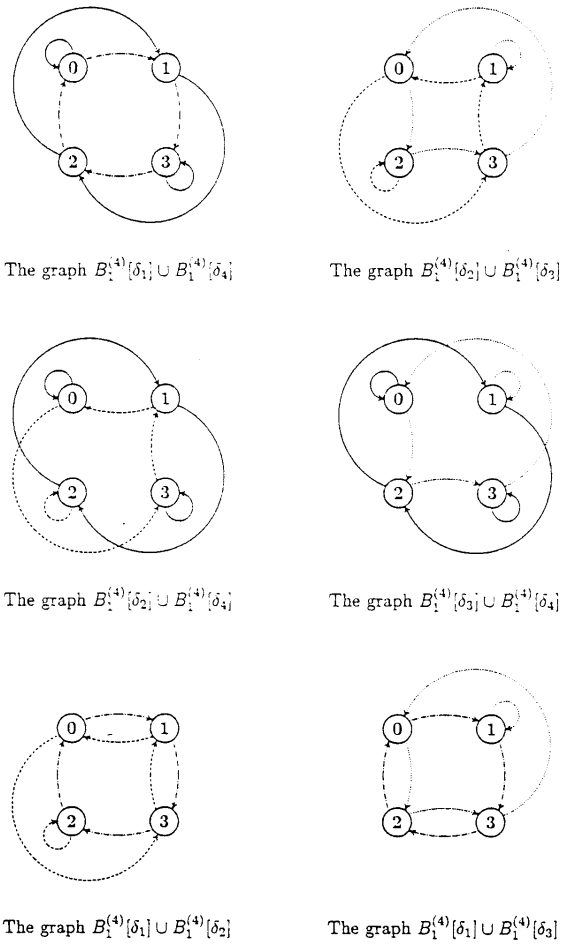


Figure 3.3. The illustration of Theorem 3.2: the connectivity of the subgraphs of the graph $B_1^{(4)}$, where δ_1, δ_2, δ_3 and δ_4 are defined in Figure 3.2

Theorem 3.4. *If a locally reducible function $\varrho \in \mathcal{C}^k_{(2)}$ is m-reducible for $m \geq 4$, then there exists such a regular function $\delta \in \mathcal{C}^k_{(m)}$ that $B^{(2)}_k[\varrho]$ is the subfactor of $B^{(m)}_k[\delta]$.*

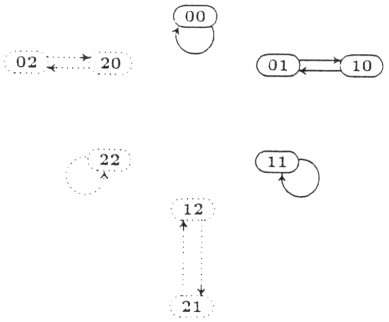


Figure 3.4. The factor $B^{(3)}_2[\vartheta]$ for $\vartheta \in \mathcal{C}^2_{(3)}$ defined by the equality $\vartheta(x_1, x_2) = x_1$; the edges and the vertices of the binary subfactor $B^{(2)}_2[\vartheta]$ are marked by the continuous lines while the other edges and vertices of $B^{(3)}_2[\vartheta]$ are marked by the dotted lines

Proof. We assume that ϱ is the m-reducible function and $\{\varrho_1, \ldots, \varrho_m\}$ is an arbitrary family colouring the graph $B^{(2)}_{k-1}$ which corresponds to ϱ. We will construct the family $\{\varrho^*_1, \ldots, \varrho^*_m\}$ consisting of such functions from $\mathcal{C}^{k-1}_{(m)}$ that

$$\varrho^*_i(x) = \varrho_i(x) \ for \ x \in Dom(\varrho_i), \quad where \ i \in \{1, \ldots, m\},$$

with

$$\varrho^*_i(x) \neq \varrho^*_j(x), \ if \ i \neq j.$$

Then $B^{(2)}_k[\varrho]$ will be a subfactor of $B^{(m)}_k[^{\mathrm{ex}}\{\varrho^*_1, \ldots, \varrho^*_m\}]$.

Let us consider an arbitrary sequence $(0, x_2, \ldots, x_{k-1}) \in \{0,1\}^{k-1}$. Then exactly such two functions ξ_1 and ξ_2 from $\{\varrho_1, \ldots, \varrho_m\}$ exist that

$$(0, x_2, \ldots, x_{k-1}) \in Dom(\xi_1) \cap Dom(\xi_2).$$

We can assume without loss of generality that $\xi_1 = \varrho_1$ and $\xi_2 = \varrho_2$. There are four possible cases:

(a) $(1, x_2, \ldots, x_{k-1}) \in Dom(\varrho_1) \setminus Dom(\varrho_2)$,
(b) $(1, x_2, \ldots, x_{k-1}) \in Dom(\varrho_2) \setminus Dom(\varrho_1)$,
(c) $(1, x_2, \ldots, x_{k-1}) \in Dom(\varrho_1) \cap Dom(\varrho_2)$,

(d) $(1, x_2, \ldots, x_{k-1}) \notin Dom(\varrho_1) \cup Dom(\varrho_2)$.

They are presented in the tables in Figure 3.5, where $a \in \{0, 1\}$ and the symbol $*$ means that the value of the corresponding function is undefined.

It is easy to see that if $m > 3$ then in each case we have considered there exists the family $\{\varrho_1^*, \ldots, \varrho_m^*\}$ which consists of the functions from $\mathcal{C}_{(m)}^{k-1}$ satisfying the above conditions. ■

Using the notations from Theorem 3.4, if $m = 3$ then $\{\varrho_1^*, \ldots, \varrho_m^*\}$ exists if and only if for each $(0, x_2, \ldots, x_{k-1})$ only (a) or (b) are the possible cases. Of course the case (d) is not possible while the case (c) is presented in the below table.

x	$\varrho_1(x)$	$\varrho_2(x)$	$\varrho_3(x)$
$(0, x_2, \ldots, x_{k-1})$	a	$\bar{a}$	$*$
$(1, x_2, \ldots, x_{k-1})$	$\bar{a}$	a	$*$
$(2, x_2, \ldots, x_{k-1})$	$*$	$*$	$*$

Theorem 3.5. *Let $\varrho \in \mathcal{C}_{(2)}^k$. If there exists such a regular function $\delta \in \mathcal{C}_{(m)}^k$ that $B_k^{(2)}[\varrho]$ is a subfactor of $B_k^{(m)}[\delta]$, then the function ϱ is t-reducible for $t \leq m$.*

Proof. Let us assume that $\varrho \in \mathcal{C}_{(2)}^k$ and the factor $B_k^{(m)}[\varrho]$ is the subfactor of the factor $B_k^{(m)}[\delta]$, where δ is a regular function from $\mathcal{C}_{(m)}^k$. Of course ϱ is the locally reducible function. Let $\{\delta_1^*, \ldots, \delta_m^*\}$ be the family of the components of the function δ. For arbitrary $i \in \{1, \ldots, m\}$ and $x \in \{0, 1\}^{k-1}$ let us put

$$\delta_i(x) = \begin{cases} \delta_i^*(x), & \text{if } \delta_i^*(x) \in \{0, 1\}, \\ \text{undefined}, & \text{otherwise.} \end{cases}$$

The family $\{\delta_1, \ldots, \delta_m\}$ can be the colouring family of the function ϱ because it satisfies the conditions (2.5)–(2.7) of Theorem 2.2, but it does not have to be the minimal family. Therefore for an arbitrary colouring family $\{\varrho_1, \ldots, \varrho_t\}$ of the locally reducible function ϱ the inequality $t \leq m$ must be satisfied. ■

Table a

x	$\varrho_1(x)$	$\varrho_2(x)$	$\varrho_3(x)$	$\cdots$	$\varrho_i(x)$	$\cdots$	$\varrho_m(x)$
$(0, x_2, \cdots, x_{k-1})$	a	$\overline{a}$	$*$	$\cdots$	$*$	$\cdots$	$*$
$(1, x_2, \cdots, x_{k-1})$	$\overline{a}$	$*$	$*$	$\cdots$	a	$\cdots$	$*$
$(2, x_2, \cdots, x_{k-1})$	$*$	$*$	$*$	$\cdots$	$*$	$\cdots$	$*$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$(m-1, x_2, \cdots, x_{k-1})$	$*$	$*$	$*$	$\cdots$	$*$	$\cdots$	$*$

Table b

x	$\varrho_1(x)$	$\varrho_2(x)$	$\varrho_3(x)$	$\cdots$	$\varrho_i(x)$	$\cdots$	$\varrho_m(x)$
$(0, x_2, \cdots, x_{k-1})$	a	$\overline{a}$	$*$	$\cdots$	$*$	$\cdots$	$*$
$(1, x_2, \cdots, x_{k-1})$	$*$	a	$*$	$\cdots$	$\overline{a}$	$\cdots$	$*$
$(2, x_2, \cdots, x_{k-1})$	$*$	$*$	$*$	$\cdots$	$*$	$\cdots$	$*$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$(m-1, x_2, \cdots, x_{k-1})$	$*$	$*$	$*$	$\cdots$	$*$	$\cdots$	$*$

Table c

x	$\varrho_1(x)$	$\varrho_2(x)$	$\varrho_3(x)$	$\cdots$	$\varrho_i(x)$	$\cdots$	$\varrho_m(x)$
$(0, x_2, \cdots, x_{k-1})$	a	$\overline{a}$	$*$	$\cdots$	$*$	$\cdots$	$*$
$(1, x_2, \cdots, x_{k-1})$	$\overline{a}$	a	$*$	$\cdots$	$*$	$\cdots$	$*$
$(2, x_2, \cdots, x_{k-1})$	$*$	$*$	$*$	$\cdots$	$*$	$\cdots$	$*$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$(m-1, x_2, \cdots, x_{k-1})$	$*$	$*$	$*$	$\cdots$	$*$	$\cdots$	$*$

Table d

x	$\varrho_1(x)$	$\varrho_2(x)$	$\cdots$	$\varrho_i(x)$	$\cdots$	$\varrho_j(x)$	$\cdots$	$\varrho_m(x)$
$(0, x_2, \cdots, x_{k-1})$	a	$\overline{a}$	$\cdots$	$*$	$\cdots$	$*$	$\cdots$	$*$
$(1, x_2, \cdots, x_{k-1})$	$*$	$*$	$\cdots$	a	$\cdots$	$\overline{a}$	$\cdots$	$*$
$(2, x_2, \cdots, x_{k-1})$	$*$	$*$	$\cdots$	$*$	$\cdots$	$*$	$\cdots$	$*$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$(m-1, x_2, \cdots, x_{k-1})$	$*$	$*$	$\cdots$	$*$	$\cdots$	$*$	$\cdots$	$*$

Figure 3.5. The illustration of the proof of Theorem 3.4

References

[1] M. Cohn and A. Lempel, *Cycle decomposition by disjoint transpositions*, J. Combin. Theory (A) **13** (1972) 83–89.

[2] E.D. Erdmann, Complexity measures for testing binary keystreams, PhD thesis, Stanford University, 1993.

[3] H. Fredricksen, *A survey of full length nonlinear shift register cycle algorithms*, SIAM Rev. **24** (1982) 195–221.

[4] E.R. Hauge and T. Helleseth, *De Bruijn sequences, irreducible codes and cyclotomy*, Discrete Math. **159** (1996) 143–154.

[5] C.J.A. Jansen, Investigations on nonlinear strimcipher systems: Construction and evaluation methods, PhD thesis, Technical University of Delft, 1989.

[6] M. Łatko, Design of the maximal factors in de Bruijn graphs, (in Polish), PhD thesis, UMCS, 1987.

[7] E. Łazuka and J. Żurawiecki, *The lower bounds of a feedback function*, Demonstratio Math. **29** (1996) 191–203.

[8] R.A. Rueppel, Analysis and design of stream ciphers (Springer-Verlag, 1986).

[9] P. Wlaź and J. Żurawiecki, *An algorithm for generating M-sequences using universal circuit matrix*, Ars Combinatoria **41** (1995) 203–216.

[10] J. Żurawiecki, *Elementary k-iterative systems* (*the binary case*), J. Inf. Process. Cybern. EIK **24** 1/2 (1988) 51–64.

[11] J. Żurawiecki, *Locally reducible iterative systems*, Demonstratio Math. **23** (1990) 961–983.

Received 21 September 1998